Indag. Mathem., N.S. 3 (2), 129–135 June 22, 1992

Commutateurs dans les groupes métabéliens

by Christophe Bavard and Gaël Meigniez

Unité de Mathématiques Pures et Appliquées, Ecole Normale Supérieure de Lyon, 46, Allée d'Italie, 69364 Lyon Cedex 07, France

Communicated by Prof. W.T. van Est at the meeting of November 25, 1991

ABSTRACT

Consider M_n the metabelian group with n generators ($n \in \mathbb{N}^*$), and denote by $c(M_n)$ the minimal number of commutators required to express an arbitrary element of the commutator subgroup $[M_n, M_n]$. We prove the following inequalities:

$$E(n/2) \leq c(M_n) \leq n$$

where E is the greatest integer function, and we study in details the case $n=2$.

Soit Γ un groupe et Γ' son premier groupe dérivé, engendré par les commutateurs. S'il existe un entier k tel que tout élément de Γ' est le produit de k commutateurs, nous noterons $c(\Gamma)$ le plus petit de ces entiers; dans le cas contraire nous poserons $c(\Gamma) = \infty$.

Par exemple $c(SL_2(\mathbb{Z}))$ est infini, tandis que $c(SL_n(\mathbb{Z}))$ est fini pour $n \geq 3$ ([8]); citons aussi [4] qui donne des résultats généraux pour les groupes linéaires des anneaux commutatifs ainsi que de nombreuses références. Il est facile de vérifier (voir par exemple [2]) que $c(\Gamma)$ est infini pour les groupes libres (différents de $\mathbb{Z}$!).

Nous étudions ici le cas des groupes *métabéliens* libres, c'est-à-dire les quotients des groupes libres par leur second groupe dérivé. Voici notre résultat principal:

THÉORÈME 1. *Soit M_n (resp. M_∞) le groupe métabélien libre à n (resp. une* *infinité dénombrable de) générateurs* $(n \geq 2)$. *Alors*:

(i) $c(M_2)=2$.

(ii) $E(n/2) \leq c(M_n) \leq n$, *où E est la partie entière.*

(iii) $c(M_\infty)=\infty$.

COROLLAIRE. $c(\Gamma)$ *est fini pour tout groupe polycyclique* Γ.

Voyons tout de suite comment le corollaire résulte du théorème. Les groupes polycycliques sont exactement les groupes résolubles dont les dérivés successifs $\Gamma', \ldots, \Gamma^{(p)}=(\Gamma^{(p-1)})'$ sont de type fini. On suppose $\Gamma^{(p+1)}=\{1\}$ et on raisonne par récurrence sur p: par hypothèse de récurrence $c(\Gamma/\Gamma^{(p)})$ est fini. Par ailleurs $\Gamma^{(p-1)}$ est métabélien de type fini, donc d'après notre théorème $c(\Gamma^{(p-1)})$ est fini. On conclut en observant que $c(\Gamma)$ est majoré par $c(\Gamma/\Gamma^{(p)})+c(\Gamma^{(p-1)})$.

REMARQUE. Ce corollaire est à rapprocher d'un résultat analogue concernant le genre des classes du deuxième groupe d'homologie $H_2(\Gamma,\mathbb{Z})$ ([1, théorème 2–2]).

La démonstration du théorème occupe le reste de cet article. Nous commençons par majorer $c(M_n)$ (§ 1). Le § 2 est consacré à l'étude de M_2. Enfin, dans le § 3 nous minorons $c(M_n)$.

1. MAJORATION DE $c(M_n)$

Le groupe M_n est défini comme quotient du groupe libre à n générateurs par son second groupe dérivé; on appellera $u_1, \ldots, u_n$ ses n générateurs naturels. Il agit par conjugaison sur le groupe abélien M_n'. L'action de M_n' sur lui-même est triviale, donc l'anneau commutatif des polynômes de Laurent $A_n=\mathbb{Z}[U_i, U_i^{-1}]_{i=1,\ldots,n}$ opère aussi sur M_n'. Ces actions seront notées $x \cdot y$ et $P \cdot y$ $(x \in M_n, P \in A_n, y \in M_n')$ et on adcptera la notation additive pour le produit de M_n'. Par exemple on a les relations:

$$(1) \qquad [y,x]=yxy^{-1}x^{-1}=(1-x)\cdot y \quad (x \in M_n, y \in M_n')$$

$$(2) \qquad [xy,z]=x\cdot[y,z]+[x,z] \qquad (x,y,z \in M_n).$$

L'égalité (2) montre que M_n' est engendré, comme A_n-module, par $\{[u_i,u_j]; 1 \leq i<j \leq n\}$. On voit aussi que les éléments du sous-groupe $[M_n', M_n]$ sont de la forme

$$(3) \qquad \sum_{i=1}^{n} (1-u_i)\cdot y_i \quad \text{où} \quad y_i \in M_n'.$$

Cela résulte de (1) et des identités polynomiales:

$$1-XY=(1-Y)+(1-X)Y, \ 1-X^{-1}=-X^{-1}(1-X).$$

Nous pouvons maintenant majorer $c(M_n)$. Vu les relations (3) et

$$(4) \qquad [xy,z]=[x,z]+[y,z]+(x-1)\cdot[y,z] \quad (x,y,z\in M_n)$$

tout élément γ de M_n' se laisse mettre sous la forme

$$\gamma=\sum_{i=1}^{n}[u_i,x_i]+\sum_{i=1}^{n}(1-u_i)\cdot y_i=\sum_{i=1}^{n}([y_i,u_i]+[u_i,x_i]) \quad (x_i\in M_n,\ y_i\in M_n').$$

Enfin, pour obtenir γ comme produit de n commutateurs, il ne reste plus qu'à regrouper les termes par paires grâce à l'identité

$$[y,x][x,z]=[yz^{-1},zxz^{-1}].$$

En particulier $c(M_2)\leq 2$.

REMARQUE. Dans le groupe libre engendré par u et v, l'élément $[u,v]^N$ est le produit de $E(N/2)+1$ commutateurs et pas moins (voir [2, 3]). Par contre, ce qui précède montre que toute puissance $[x,y]^N$ $(x,y\in M_n, N\in\mathbb{Z})$ est toujours le produit de deux commutateurs de M_n (faciles à expliciter).

2. COMMUTATEURS DANS M_2

Dans ce paragraphe, nous établissons un critère qui caractérise les commutateurs de M_2. En fait, ce paragraphe et le précédent fournissent un algorithme pour écrire chaque élément de M_2' comme un produit explicite de commutateurs aussi court que possible.

Soient u et v les générateurs de M_2. Tout élément γ de M_2' est de la forme:

$$\gamma=P\cdot[u,v] \quad \text{avec } P\in\mathbb{Z}[U^{\pm 1},V^{\pm 1}]$$

et cette écriture est unique. Pour nous en convaincre, choisissons deux réels λ, μ algébriquement indépendants sur le corps des rationnels, et considérons la représentation ϱ de M_2 dans le groupe des homothéties-translations de $\mathbb{R}$ définie par $\varrho(u)(t)=\lambda t$ et $\varrho(v)(t)=\mu t+1$. Le commutateur $[\varrho(u),\varrho(v)]$ est une translation d'amplitude $c\neq 0$. L'image de $P\cdot[u,v]$ est la translation d'amplitude $P(\lambda,\mu)c$. Si bien que $P\cdot[u,v]=1$ entraîne $P=0$.

Remarquons que γ appartient à $[M_2,M_2']$ si et seulement si P appartient à l'idéal de $\mathbb{Z}[U^{\pm 1},V^{\pm 1}]$ engendré par $1-U$ et $1-V$. En d'autres termes $P(1,1)$ représente la classe de γ modulo $[M_2,M_2']$.

Considérons $T=\{(\zeta,\omega)\in\mathbb{C}\times\mathbb{C}/|\zeta|=|\omega|=1\}$, $Z(P)$ l'ensemble des zéros de P dans T, et $\tilde{Z}(P)=Z(P)\cup\{(1,1)\}$. Faisons d'abord une remarque qui éclairera le sens de notre théorème.

REMARQUE. Soient $P\in\mathbb{Z}[U^{\pm 1},V^{\pm 1}]$ et G un sous-groupe de T contenu dans $\tilde{Z}(P)$. Si G est fini, alors $P(1,1)$ est divisible par l'ordre de G. Si G est infini, alors $P(1,1)=0$.

PREUVE. Si G est fini, associons à chaque polynôme Q sa moyenne sur les orbites de G, c'est-à-dire le polynôme:

$$Q^*(U,V)=|G|^{-1}\sum_{(\zeta,\omega)\in G} Q(\zeta U,\omega V).$$

On vérifie immédiatement que la moyenne de tout monôme U^pV^q est soit 0, soit U^pV^q. Il en résulte que Q^* est à coefficients entiers. En particulier, $P(1,1)=|G|P^*(1,1)$ est divisible par $|G|$.

Si G est infini, alors $Z(P)$ s'accumule sur $(1,1)$, donc $P(1,1)=0$.

THÉORÈME 2. *Soit $\gamma=P\cdot[u,v]$ un élément de M_2'. Supposons que $\gamma\notin[M_2,M_2']$ (resp. $\gamma\in[M_2,M_2']$). Alors γ est un commutateur si et seulement si $\tilde{Z}(P)$ contient un sous-groupe fini d'ordre $|P(1,1)|$ (resp. contient un sous-groupe à un paramètre de T).*

Les commutateurs sont donc caractérisés par le fait que $\tilde{Z}(P)$ contient un sous-groupe de T aussi grand que possible. Voici quelques corollaires de ce théorème.

1. Si $P(1,1)=\pm 1$ alors $P\cdot[u,v]$ est toujours un commutateur.
2. Aucune puissance γ^k, où $\gamma\notin[M_2,M_2']$ et $k\geq 2$, n'est un commutateur.

En effet, écrivons $\gamma=P\cdot[u,v]$: si γ^k était un commutateur, $\tilde{Z}(kP)$ contiendrait un sous-groupe de T d'ordre $k|P(1,1)|$. Comme $\tilde{Z}(P)=\tilde{Z}(kP)$, l'entier $k|P(1,1)|$ diviserait $|P(1,1)|$ (remarque précédant le théorème 2), ce qui est contradictoire.

3. En particulier $[u,v]^2$ n'est pas un commutateur, ce qui achève de démontrer que $c(M_2)=2$.

PREUVE DU THÉORÈME 2. Supposons d'abord que γ est un commutateur: $\gamma=[\alpha u^pv^q,\beta u^rv^s]$, où $p,q,r,s\in\mathbb{Z}$ et $\alpha,\beta\in M_2'$.

On a alors $ps-qr=P(1,1)$. En effet, comme le crochet [,] est bilinéaire modulo $[M_2,M_2']$ (Eq. (4)), l'élément γ est congru à $(ps-qr)[u,v]$ modulo $[M_2,M_2']$.

Soit G le sous-groupe des éléments (ζ,ω) de T solutions de $\zeta^p\omega^q=\zeta^r\omega^s=1$. Quand $ps-qr$ est non nul, G est fini d'ordre $|ps-qr|$. Quand $ps-qr$ est nul, G contient un sous-groupe à un paramètre de T.

Montrons que $P(\zeta,\omega)=0$ pour tout élément (ζ,ω) de G autre que $(1,1)$. Soit ϱ la représentation de M_2 dans le groupe des isométries affines de $\mathbb{C}$ définie par

$$\varrho(u)(z)=\zeta z+1-\bar{\omega}\quad\text{et}\quad\varrho(v)(z)=\omega z+\bar{\zeta}-1.$$

Puisque $\zeta^p\omega^q=\zeta^r\omega^s=1$, les isométries $\varrho(\alpha u^pv^q)$ et $\varrho(\beta u^rv^s)$ sont deux translations, donc commutent: $\varrho(\gamma)=id$. Mais comme $\varrho(\gamma)$ est une translation d'amplitude $P(\zeta,\omega)(|\zeta-1|^2+|\omega-1|^2)$, on a nécessairement $P(\zeta,\omega)=0$.

Pour établir la réciproque, commençons par le cas où $\gamma\notin[M_2,M_2']$. Supposons que $\tilde{Z}(P)$ contient un sous-groupe G d'ordre $|P(1,1)|$. Ce sous-groupe fini peut être décrit comme l'ensemble des solutions de $\zeta^p\omega^q=\omega^s=1$, où p,q,s sont trois entiers avec p et s positifs vérifiant $ps=|P(1,1)|$.

Soit Q le polynôme défini par $[u^pv^q,v^s]=Q\cdot[u,v]$. D'après le raisonnement précédent, Q vaut ps en $(1,1)$ et 0 en tout autre point de G. Donc $P-Q$ est nul sur G.

Montrons maintenant que l'idéal de $\mathbb{Z}[U^{\pm 1}, V^{\pm 1}]$ formé des polynômes nuls sur G est l'idéal engendré par $1-U^pV^q$ et $1-V^s$. Soit S un polynôme de Laurent nul sur G. A un monôme près, S est égal à un polynôme usuel; effectuons la division euclidienne de S par $1-U^pV^q$ dans l'anneau $(\mathbb{Z}[V^{\pm 1}])[U]$, puis la division du reste (à un monôme près) par $1-V^s$; le nouveau reste R est congru à S modulo $(1-U^pV^q, 1-V^s)$ et s'écrit

$$\sum_{0\le i\le p-1} R_i(V)U^i, \quad \text{où } R_i\in\mathbb{Z}[V] \text{ et degré}(R_i)<s.$$

Pour chaque ω racine s-ième de l'unité, les $R_i(\omega)$ $(i=0,\dots,p-1)$ sont nuls car $S(U,\omega)$ admet p racines. Comme degré$(R_i)<s$, les R_i sont nuls, i.e. $R=0$.

Il existe donc $A,B\in\mathbb{Z}[U^{\pm 1}, V^{\pm 1}]$ tels que:

$$P=Q+A(1-V^s)-B(1-U^pV^q)$$

En d'autres termes, si l'on note $\alpha=A\cdot[u,v]$ et $\beta=B\cdot[u,v]$, on a d'après les relations (1) et (2): $\gamma=[u^pv^q,v^s]+[\alpha,v^s]+[u^pv^q,\beta]=[\alpha u^pv^q,\beta v^s]$.

Dans le cas où $\gamma\in[M_2,M_2']$, on suppose que $Z(P)\cap T$ contient un groupe à 1 paramètre. Il existe donc deux entiers p,q tels que $Z(P)$ contient l'ensemble des solutions de $\zeta^p\omega^q=1$. On montre (comme plus haut) que l'idéal des polynômes de Laurent nuls en ces points est l'idéal engendré par $1-U^pV^q$. En particulier il existe $A\in\mathbb{Z}[U^{\pm 1}, V^{\pm 1}]$ tel que $P=A(1-U^pV^q)$, d'où $\gamma=[A\cdot[u,v],u^pv^q]$.

3. MINORATION DE $c(M_n)$

Nous allons minorer $c(M_n)$ en nous ramenant à un problème d'algèbre linéaire, grâce à la proposition suivante qui a son propre intérêt:

PROPOSITION. *Soit M un groupe métabélien libre. On note $\bar{M}=M/M'$ son abélianisé et $\Lambda^2_{\mathbb{Z}}(\bar{M})$ la deuxième puissance extérieure de $\bar{M}$. Alors il existe un morphisme de groupes abéliens $M'\to\Lambda^2_{\mathbb{Z}}(\bar{M})$ qui envoie $[x,y]$ sur $\bar{x}\wedge\bar{y}$ $(x,y\in M)$.*

Montrons tout de suite comment cette proposition entraîne l'inégalité $c(M_n)\ge E(n/2)$, qui achève la preuve du théorème 1. Posons $k=E(n/2)$; on a dans l'algèbre extérieure de $\bar{M}_n$:

$$\Big(\sum_{i=1}^{k}\bar{u}_{2i-1}\wedge\bar{u}_{2i}\Big)^k=k!\,\bar{u}_1\wedge\bar{u}_2\cdots\wedge\bar{u}_{2k},$$

qui est non nul, contrairement à la puissance k-ième de toute somme du type $\sum_{1\le i\le p}\bar{x}_i\wedge\bar{y}_i$ avec $p<k$. Il faut donc, d'après la proposition, au moins k commutateurs de M_n pour décomposer $[u_1,u_2][u_3,u_4]\cdots[u_{2k-1},u_{2k}]$.

Soit maintenant le groupe métabélien libre M_∞ engendré par $\{u_i; i\in\mathbb{N}\}$. Ce qui précède montre que $c(M_\infty)=\infty$.

PREUVE DE LA PROPOSITION. Comme nous l'a fait remarquer J. Barge, la proposition peut s'établir par des considérations cohomologiques. Nous avons choisi d'utiliser le plongement de Magnus (voir [7]), ce qui est bien naturel quand on étudie les commutateurs.

Etant donné un ensemble d'indices I, considérons l'algèbre des séries formelles à coefficients entiers en les indéterminées *non commutatives* U_i ($i \in I$). Le groupe libre L de base $\{u_i; i \in I\}$ admet un plongement φ dans le groupe des éléments inversibles de cette algèbre, plongement défini par:

$$\varphi(u_i) = 1 + U_i$$

(voir [7, p. 310]). Pour tout élément x de L, on notera $\varphi(x) = 1 + X$ et $X_{(k)}$ la partie homogène de degré k ($k \geq 1$) de $1 + X$: ainsi $X_{(1)}$ est l'abélianisé $\bar{x}$ de x. Pour $k = 2$ on a la relation:

$$\{(1 + X)(1 + Y)\}_{(2)} = X_{(2)} + Y_{(2)} + X_{(1)} Y_{(1)}.$$

Comme de plus $X_{(1)} = 0$ si $x \in L'$, l'application $x \to X_{(2)}$ restreinte à L' est un morphisme. Par ailleurs on vérifie la formule:

$$[1 + X, 1 + Y] = 1 + \sum_{p,q=0}^{\infty} (-1)^{pq}(XY - YX)X^p Y^q,$$

en particulier

$$[1 + X, 1 + Y]_{(2)} = X_{(1)}Y_{(1)} - Y_{(1)}X_{(1)}.$$

Ainsi la partie homogène de degré 2 définit un morphisme ϕ_2 de $M' = L'/L''$ dans $\otimes^2_{\mathbb{Z}} \bar{M}$, vérifiant $\phi([x, y] = \bar{x}\bar{y} - \bar{y}\bar{x}$.

Le morphisme ϕ cherché est obtenu en composant ϕ_2 avec la projection de $\otimes^2_{\mathbb{Z}} \bar{M}$ sur $\Lambda^2_{\mathbb{Z}} \bar{M}$ et en divisant par 2.

Quelques commentaires s'imposent. Le corollaire $c(M_\infty) = \infty$ nous semble intéressant pour deux raisons.

Tout d'abord il y a une condition générale pour un groupe Γ qui implique $c(\Gamma) = \infty$: c'est l'existence de certaines classes non nulles dans le deuxième groupe de cohomologie *bornée* de Γ (voir [2] pour les détails); cette condition ne s'applique pas à M_∞ car les groupes résolubles ont une cohomologie bornée triviale ([5] ou [6]). La preuve de $c(M_\infty) = \infty$ qui précède est donc de nature différente.

Par ailleurs tout groupe résoluble R (de type fini ou non) satisfait une propriété plus faible que c fini ([2]): si $c(\gamma)$ désigne le nombre minimal de commutateurs pour décomposer un élément γ de R', alors

$$\lim_{p \to \infty} \frac{c(\gamma^p)}{p} = 0 \quad (\forall \gamma \in R').$$

Cette propriété est aussi reliée à la cohomologie bornée.

La question qui semble intéressante maintenant est de décider si $c(\Gamma)$ est fini ou non pour les groupes résolubles (ou même moyennables) de type fini.

BIBLIOGRAPHIE

1. Barge, J. et E. Ghys – Surfaces et cohomologie bornée. Invent. Math. **92,** 509-526 (1988).
2. Bavard, C. – Longueur stable des commutateurs. L'enseignement Math. **37,** 109-150 (1991).
3. Culler, M. – Using surfaces to solve equations in free groups. Topology **20,** 133-145 (1981).
4. Dennis, R.K. and L.N. Vaserstein – On a question of M. Newman on the number of commutators. J. of Algebra **118,** 150-161 (1988).
5. Gromov, M. – Volume and bounded cohomology. Pub. Math. IHES **56,** 5-99 (1982).
6. Ivanov, N.V. – Foundations of the theory of bounded cohomology. J. of Soviet Math. **37,** 1090-1115 (1987).
7. Magnus, W., A. Karras and D. Solitar – Combinatorial group theory. Dover (1976).
8. Newman, M. – Unimodular commutators. Proc. AMS **101 n° 4,** 605-609 (1987).